ACEEE Int. J. on Signal and Image Processing , Vol. 4, No. 3, Sept 2013

Authentication of Degraded Fingerprints Using Robust Enhancement and Matching Techniques

O. A. Esan[1], S.M. Ngwira[2], and T. Zuva[3]
[1, 2, 3] Tshwane University of technology/Computer System Engineering, Pretoria, South Africa
esanoa@tut.ac.za, ngwiraSM@tut.ac.za, ZuvaT@tut.ac.za

***Abstract*—Biometric system is an automated method of identifying a person based on physiological, biology and behavioural traits. The physiological traits in include face, fingerprint, palm print and iris which remains permanent throughout an individual life time. In the event that these physiological traits have been degraded then the authentication of an individual becomes very difficult. The challenge of restoring a degraded physiological image to an acceptable appearance in order to authenticate an individual is very enormous. Fingerprint is one of the most extensively used biometric systems for authentication in areas where security is of high importance. This is due to their accuracy and reliability. However, extracting features out of degraded fingerprints is the most challenging in order to obtain high fingerprint matching performance. This paper endeavors to enhance the clarity of fingerprint minutiae, removing false minutiae and improve the matching performance using a robust Gabor Filtering Technique (GFT) and Back Propagation Artificial Neural Network (BP-ANN). The experiments showed a remarkable improvement in the performance of the system.**

***Index Terms*—first term, second term, third term, fourth term, fifth term, sixth term**

I. Introduction

The need for higher security accuracy has led to rapid popularity and acceptance of biometric authentication and verification system. Biometric system is referred to as an automated method of identifying a person based on physiological, biological and behavioural traits. The physiological traits include face, fingerprint, palm print and iris which remain permanent throughout individual's life time. The biological traits are signature, gait, speech and keystroke, etc and the behavioural traits e.g., signature, grait etc. which cannot change with time [1, 4].

Among all the biometric system, fingerprint is one of the most widely used biometric for authentication security. This is because of the distinctive characteristics such as uniqueness, permanence, immutability and high accuracy performance [4]. In fingerprint, minutiae (ridge ending and valley bifurcations) are the most commonly and acceptable feature used by FBI and forensic for identification of criminals and detecting perpetrators [4, 9].

In fingerprint authentication system, there are two procedures of performing personal confirmation; (i) the verification procedure which involves matching of one fingerprint with another fingerprint (one to one match) and (ii) identification procedure which are one to many match [1].

However, most fingerprint matching authentication system are experiencing fair matching performance due to degradation in fingerprint images might be as a result of accident, wrinkles, occupation and skin elasticity, Since the matching performance of fingerprint authentication system relies heavily on the quality of inputted fingerprint [5,7].

A. Degraded Fingerprints

Fingerprint images consist of minutiae features which are a combination of ridge and valley. However, due to some number of factors (such as aberrant formations of epidermis ridges of fingerprint, occupational mark, problem with acquisition devices etc), the ridges and valley structure may not always be well defined [5]. A typical example of fingerprint with degradation is shown in Fig.1.

Figure 1. Fingerprints with degradation

This has a greater significant on the matching performance of authentication system as the system might reject the authorized system users and accept unauthorized users.

B. Matching Fingerprint

Obviously, the performance in minutia-based matching depends on quality of inputted fingerprint may not be well defined as a result of poor device image acquisition, displacement and distortion due the registration stage. Due to different properties of fingerprint sensor and different conditions under which a fingerprint is captured, the quality of fingerprint image can vary greatly and create a numerous false minutiae in fingerprint [6].

The features extracted from the input fingerprint with the combined features stored in the template database are often not the same during matching due to several processes that minutiae-based algorithm undergo [1]. Fig 2(a) shows a query fingerprint which fails to match with the same fingerprint database template in Fig 2(b).

Figure 2. (a) query fingerprint (b) database template

DOI: 01.IJSIP.4.3.1316

The noise and some spurious minutiae makes Fig 2a not to correspond to Fig 2b, and subject user authentication to rejection errors. Thus, it is of a special relevance to address these issues for the benefit of fingerprint authentication users. The major contributions of this paper are as follows:

- Addressing the issue of fingerprint degradation with a Gabor Filtering technique
- Analysing theoretically the issue of false minutia from the reliable minutiae and integrated artificial neural network to improve fingerprint matching performance.
- Addressing issue of time search in large data using GFT-BPANN.

The rest of this paper is organized as follows: section 2 presents an overview of fingerprint authentication system, section 3 is the proposed fingerprint authentication system, section 4 describe the experimental result, section 5 conclude the paper and section 6 Acknowledgement and References.

II. Theoretical Background

A. Related Works

Various techniques have been used in literature for improving the grey level of fingerprint image. According to [3], a fingerprint enhancement with a contextual filter are unreliable in the areas corrupted by noise and introduced a scale theory for enhancement process. They decomposed fingerprint into a series of images and organized the images by courser to finer scheme, the globe and interpolation is used to eliminate the influence of noise to the largest extent. Their experimental result revealed that the algorithm is fast and can improve the performance of fingerprint verification system.

Also [11], proposed image enhancement for fingerprint minutiae-based using Contrast Limited Adaptive Histogram Equalization (CLAHE), standard deviation and sliding neighborhood was proposed. They used CLAHE with Clip Limit in order to enhance the contrast of small tiles, to eliminate the artificially introduced boundaries and to avoid over-saturation of the image specifically in homogeneous areas, and also combined filters in both spatial and Fourier domains to obtain proper enhanced image. Finally a slide neighborhood processing was applied to clarify the minutiae.

The research in [2], presents fingerprint enhancement by shape adaptation and scale selection based on two mechanisms to enhance fingerprint image. The shape adaptation procedure adapts the smoothing operation to the local ridges structures, which allows interrupted ridges to join without destroying the essential singularities. The scale selection procedure estimates local ridge width and adapts the amount of smoothing to the local amount of noise. However, the combined approach makes it possible to resolve fine scale structure in clear areas while reducing the risk of enhancing noise in blurred or fragmented areas.

Histogram equalization defines a mapping of grey-levels P into grey-levels q such that the distribution of grey-level is uniform [1]. This mapping stretches contrast for grey-levels near the histogram maxima. Since contrast is expanded for most of the image pixel, the transformation improves the detectability of many features [1, 3].The key advantage of this technique is that it is fairly straight forward and an invertible operation. Also in the theory, if the histogram equalization function is known then the original histogram can be recovered easily. The calculation is not computational intensive. The disadvantage of this approach is that it is indiscriminate.

A structure-adaptive anisotropic filtering in the space domain using both local intensity, orientation and an anisotropic measure to control the shape of the filter instead of using local gradient and anisotropic measure to control the anisotropic of filter was proposed in [1,15].

Despite the structural-adaptive filter is directional and adjust the shape of the kernel according to the image anisotropic local features; the filter caused to unnecessary blurring in processed image due to the linearity of its filtering function. The structure-adaptive anisotropic filter operated on pixel neighborhood of a constant size, which is not depending on local features of input image [15]. A solution was suggested in [1,15] on these problems with improved structure-adaptive anisotropic filter, which combines non-linear filtering function, a more robust to noise technique for oriented pattern direction estimation and elliptical kernel with its form, size and direction depending on image local anisotropic features.

The Merits of this technique is it has a frequency and orientation which helps to remove undesired noise and also preserve ridge and valley structure. The demerit of the approach is it is computationally intensive.

However, apart from the above mentioned methods, this study proposes a GFT-BPANN approach to address the degraded fingerprint and matching based on Gabor Filtering and Back Propagation Artificial Neural Network in [1,5].

B. Gabor Filtering Technique (GFT)

Computer image processing utilizes Gabor function for analyzing image texture, due to frequency selective property and orientation selective property [7, 17]. With the selective property exhibited by GFT the fingerprint image and invariant coordinates for ridges in the local neighborhood are defined, and the selective orientation property helps in modeling the grey level along the ridges and valleys into a sinusoidal-shape wave the area in fingerprint where there is no appearance of minutiae [4,7]. Thus, an even-symmetric real component of 2–D Gabor as in (1) can be used removing noise and preserve true ridge/valley structure in fingerprint image

$$G(x, y, f_0, \theta) = e^{x} * \cos(y) \quad (1)$$

Where x on the exponential is represented as:

$$x = -\frac{1}{2} * \left[\frac{x_0^2}{\sigma_x^2} + \frac{y_0^2}{\sigma_y^2} \right] \quad (2)$$

From equation (1) and (2), θ is the ridge respected to vertical axis, f_0 is the selected ridge frequency in x_θ direction, σ_x and σ_y are the standard deviation of Gaussian function along the x_θ and y_θ axes respectively. However,

DOI: 01.IJSIP.4.3.1316

in GFT approach a pixel-wise scheme is used to estimate the orientation field of degraded fingerprint image correctly as in (3).

$$\theta_{(i,h)} = \frac{1}{2} \frac{\left(\sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} 2G_x(u,v)G_y(u,v) \right)}{\left(\sum_{v=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{u=j-\frac{w}{2}}^{j+\frac{w}{2}} G_x{}^2(u,v) - G_y^2(u,v) \right)} \quad (3)$$

w is the image block size; G_x and G_y are the gradient at each (x, y) in each block.

Thus, equation (1) is used to remove noise from degraded fingerprint since this contains useful information for enhancement. This GFT algorithm is best suited for enhancing fingerprint image with degradation.

C. Back Propagation Artificial Neural Network (BP-ANN)

Neural network consists of 3 layers cluster, input layer, output layer and hidden layer which is shown in Fig. 3. The number of clusters in these layers is 1-X Y-3, that is one cluster in the input layer, X cluster in the first hidden layers, and the two clusters in the output layer [1, 8]. Expressed mathematically as in (4):

$$a_{m,n}(t+1) = F\left(\left(\sum_{i=-s}^{s} \sum_{j=s}^{s} h_{i,j} a_{m+1}, n+j(t) \right) \right) + b \quad (4)$$

Where $h_{i,j}$ is the weight mask for pixel size $S * S$, b is the scale bias value, F is the non-linear activation function, t is the iteration step, and $a_{mn}(t+1)$ and $a_{mn}(t)$ are output and input respectively. The input image is defined as in (5).

$$a_{m,n}(0) = P \quad (5)$$

Where P is the entire input image

The activation function for non-linear piecewise function is expressed as in (6).

$$f(x) = \begin{cases} -1 & x \le -1 \\ x & -1 < x < 1 \\ 1 & x \ge 1 \end{cases} \quad (6)$$

With the initial values for the weight and biased are selected randomly. The error (E) function is defined by the actual output $a_{m,n}(t+1)$ and desired output, $d_{m,n}$ as in (7).

$$E = \frac{1}{2} \sum_m \sum_n (a_{m,n}(t+1) - d_{m,n})^2 \quad (7)$$

The benefit of this approach is, it can be used for one-to many matching fingerprint in large database. It also has a less computation time in both feature extraction and matching stages.

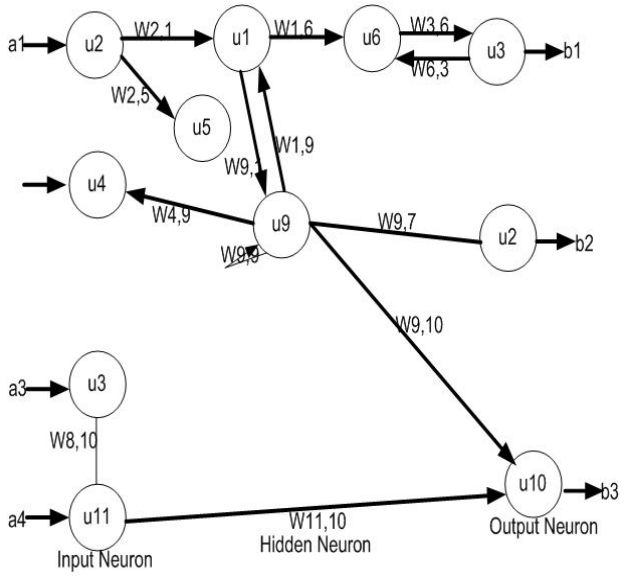

Figure 3. Artificial Neural Network Approach [8,17]

III. Proposed System Model

The system model proposed in Fig. 4 is divided into two modules namely:

(i) enrolment module
(ii) authentication module

A.Enrolment Module

From Fig. 4, the fingerprint images are acquired with a fingerprint scanner before it passes through the image enhancement stages for clarity modification.

B.Image Enhancement

Image enhancement is the process improving the quality of a digitally stored image by manipulating the image with software. It is quite easy, to make an image lighter or darker, or to increase or decrease contrast [14] [15].

C.Normalization

The process of normalization in fingerprint helps in reducing the light intensity along the ridges and valleys during sensor capturing. This is done by means of adjusting the grey-level values to predefined constant mean and variance [5].

Let $I(i, j)$ denotes the grey-level at pixel (i, j), M and Var denote the estimated mean and variance of I respectively, $G(i, j)$ denotes the normalized grey-level at pixel (i, j). M_0 and Var_0 are desired mean and variance value respectively. The normalized image is defined as given in (8).

$$G(i,j) = \begin{cases} M_0 + \sqrt{\frac{Var_0 (I(i,j) - M)}{Var}} & if\ I(i,j) > M \\ M_0 - \sqrt{\frac{Var_0 (I(i,j) - M)}{Var}} & otherwise \end{cases} \quad (8)$$

DOI: 01.IJSIP.4.3.1316

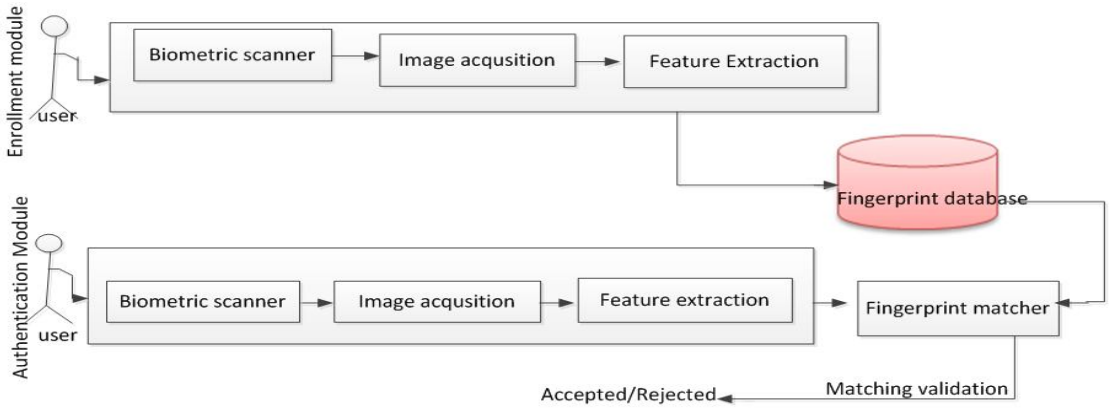

Figure 4. Optimized Fingerprint Authentication System

D.Segmentation

In any fingerprint enhancement algorithm segmentation is always treated as the first step. Segmentation is the process of separating the foreground region in fingerprint image from the background regions. The foreground is corresponding to the clear fingerprint area containing the ridges and valleys, which are the area of interest. The background corresponds to the regions outside the borders of the fingerprint area, which do not contain any valid fingerprint information [4].

The variance threshold method is used to perform segmentation by dividing the image into blocks and the grey-scale variance for each block in the image is calculated as in (9).

$$V(K) = \frac{1}{w^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}(I(i,j) - M(K))^2 \quad (9)$$

Where $V(K)$ is the variance for block k, $I(i,j)$ is the grey-level value at pixel (i,j) and $M(K)$ is the mean grey-level value for the block K.

If the variance is less than the global threshold, the block is assigned to be a background region; otherwise, it is assigned as foreground.

E. Thinning

During this stage, the characterization of each fingerprint feature is carried out by determining the value of each pixel using algorithm in [11]. The neighbourhood of the pixel that have maximum values in a sequential process obtaining a characteristics pixel value for each feature set each step due to false H breaks and lonely points which could appear in the fingerprint images. The objectives of thinning algorithm are [13, 16]:

(i) To obtain a skeletonized fingerprint image with a single pixel width and no discontinuities

(ii) To eliminate the noise and singular pixel

However, fingerprint need to be classified to distinguish between reliable and spurious minutia [10].

F. Minutiae Classification

Spurious minutiae can affect the matching accuracy of a fingerprint authentication system. If they are not well addressed it can be mis-identified as a genuine minutiae. The Fig. 5 and 6 show example of a false minutiae

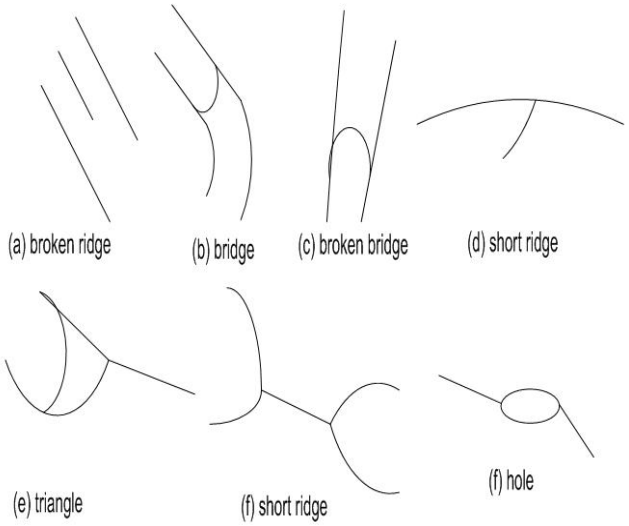

Figure 5: False Minutiae

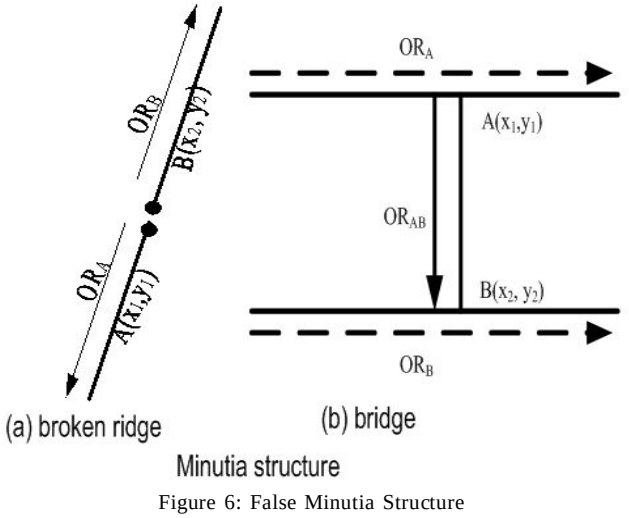

Figure 6: False Minutia Structure

However, a ridge may break into two ridges creating two endpoints as a result of scars and insufficient fingerprint pressure on the input device. Thus, these two endpoints are considered as a false minutia and must be eliminated.

DOI: 01.IJSIP.4.3.1316

There are rules for identifying false minutiae

(i) Two ends of ridges are classified as a broken ridge in Fig. 5

$$D_{AB} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \le Dist_1. \quad (10)$$

Where $Dist_1$ is a pre-specific constant

(ii) The line constructed by connecting two endpoints and two ridges connected with each minutia should flow in the same direction as in (11).

$$\theta_{ab} = \tan^{-1}\left(\frac{y_2 - y_1}{x_2 - x_1}\right) \neq \frac{1}{2}(OR_A - OR_B). \quad (11)$$

(iii) Two ridges should be flowing to the opposite direction without being connected. In Fig. 5, if ridges connected with minutia A flows downwards, the other ridge should flow upwards and minutiae B should be placed above the minutia A.

G.. Detecting Bridge Structure

Due to excessive fingerprint pressure or noise in the image, two separate ridges are sometimes connected by a short ridge to make a bridge structure. Based on this fact that ridges in fingerprint flow smooth and neighbor ridges flow in similar direction, method for detecting two fingerprint bifurcations associated with ridges structures is as follows. Fig. 6

(i) Start tracking three ridges connected to bifurcation (point A)

(ii) If one of the tracked ridges meet another bifurcation (point B), calculate orientation of the ridge connected by two bifurcations (OR_{AB}) and distance of two bifurcations $(Dist_{AB})$

(iii) If the $Dist_{AB}$ is less than a threshold value of $(Dist_2)$ and the difference between OR_{AB} and the average orientation of two bifurcations (OR_A, OR_B) is larger than a specified angle, and then two bifurcations are identified as a bridge structure.

H. Detecting Short Ridge Structure

All short ridges should be considered as false minutiae they are usually artifacts introduced by image preprocessing procedure such as ridge segmentation and thinning. The short ridge structures are detected in the following ways:

(i) Start tracking ridges from ridge ending. If a tracked ridge meets another end point or a bifurcation with in a distance $(Dist_3)$, two minutiae are considered as false.

(ii) If bifurcation meets another bifurcation while tracking ridges and two flows in opposite direction Fig. 6, two bifurcations are considered false minutia.

I. Detecting Hole Structure

The hole structure occurs due to pores and dirt on fingerprints. The hole structure can be detected in the following ways:

(i) By tracking three ridges connected to an extracted bifurcation.

(ii) If two tracked ridges meet to form another bifurcation and two bifurcations are within a distance ($Dist_4$), then both bifurcations are considered as a false minutia.

K.Feature Extraction

After the image has passed through the image enhancement stages. The next stage is extraction of fingerprint feature. However, there are many features on fingerprint, thus during the extraction the fingerprint features are represented as either ridge ending or valley bifurcation using the CN concepts concept proposed in [10] as in (12).

$$N = \frac{1}{2}\sum_{i=1}^{8} |p_i - p_{i+1}|. \quad (12)$$

Where p_i is the binary pixel value in the neighborhood of P with $pi = (0 or 1)$ and $P_9 = P_1$.

(iii) If the central pixel is 1 and has only 1 value neighbor, then the central pixel is a ridge ending as shown in Table 1.

TABLE I: RIDGE ENDING

0	0	0
0	1	0
0	0	1

(iv) If the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is ridge branch as shown in Table.2.

TABLE 2: RIDGE BRANCH

0	1	0
0	1	0
0	0	1

L. Database

After extracting valid minutiae points from inputted fingerprint image. The extracted ridge ending and bifurcation are represented in the form of x-coordinate and y-coordinate for proper storage and matching in the fingerprint database.

M.Authentication Module

Also, during the authentication stage, it requires the query fingerprint to pass again through image processing stages as in Fig. 4. The fingerprint matching algorithm is responsible for generating a similarity score from a query fingerprint and the template fingerprint. After the similarity is obtained, the comparison score is made by setting a threshold to certain value to state whether both query fingerprint and template fingerprint are from the same person [4, 12]. In order to improve the matching performance for a degraded fingerprint and even a larger database, a back propagation neural network is employed [1].

DOI: 01.IJSIP.4.3.1316

Pool of Pseudo Code for GFT-BPANN approach

ALGORITHM 1: Fingerprint Segmentation For GFT-BPANN

INPUT: Image G (i, j)
OUTPUT: Foreground

STEP 1: Divide G image into W*W
STEP 2: for each grey image (i,j)
STEP 3: estimate the grey-image variance of V (i,j) of each

$$V(K)=\frac{1}{w^2}\sum_{i=0}^{W-1}\sum_{j=0}^{W-1}(I(i,j)-M(K))^2$$

STEP 4: compute image as background
STEP 5: if variance less than threshold, otherwise
STEP 6: compute image as foreground

ALGORITHM 2: False Minutiae for GFT-BPANN

INPUT: Minutiae image
OUTPUT: Detecting broken ridge

STEP 1: for minutiae image A, B
STEP 2: calculate the Euclidean distance (D_{AB})
STEP 3: if D_{AB} is less than pre-specific distance constant ($Dist_1$)
STEP 4: if θ_{AB} is not equal to angle line in minutiae A and B
STEP 5: if the ridges direction of A and B flow opposite without connected
STEP 6: compute broken ridge

ALGORITHM 3: Short Ridge Structure for GFT-BPANN

INPUT: Minutiae image
OUTPUT: Short ridge structure

STEP 1: input image G
STEP 2: calculate distance $DIST_3$
STEP 3: if tracked ridge meet is within $DIST_3$
STEP 4: if bifurcation meet another bifurcation and two flows in opposite direction
STEP 5: compute short ridge ending

ALGORITHM 4: Bridge Structure for GFT-BPANN

INPUT: Minutiae image
OUTPUT: Detecting bridge structure

STEP 1: input minutia image G (with point A, B)
STEP 2: track three ridges connected to bifurcation (point A)
STEP 3: if one of the tracked ridges meets another bifurcation (point B),
STEP 4: calculate orientation of the ridge connected by two bifurcations (OR_{AB})
STEP 5: calculate distance of two bifurcations ($Dist_{AB}$)
STEP 6: if the $Dist_{AB}$ is less than a threshold value of ($Dist_2$)
STEP 7: if the difference between OR_{AB} < a specified angle
STEP 8: if the average orientation of two bifurcations (OR_A, OR_B) < a specified angle.
STEP 9: compute bridge structure

ALGORITHM 5: Back Propagation Neural Network

INPUT: Matrices of image $M \times N$
OUTPUT: Average feature

STEP 1: initialize the weight
STEP 2: repeat set $x_1^0,.....x_{M_0}^0$ equal to feature set off sample 1 to N
STEP 3: compute $x_i^{(k+1)}=\left(\sum_{i=0}^{MK} w_{i,j}^{(k+1)}x_i^{(k)}\right)$
STEP 4: for k = 0,..., k − 1
STEP 5: for node j = 1
STEP 6: for layers k = k − 1,...1
STEP 7: Compute

$$\delta_i^{(k)}=x_i^{(k)}\left(1-x_i^{(k)}\right)\left(\sum_{j=1}^{M_{k+1}} w_{i,j}^{(k+1)}\delta_j^{(k+1)}\right)$$

STEP 8: for $i=1,.....,M_k$
STEP 9: Replace $w_{i,j}^{(k)}$ by $w_{i,j}^{(k)}-cx_i^{(k-1)}\delta_j^{(k)}$ for i, j, k
STEP 10: Repeat step 2 and 9 until weights $w_{i,j}^{(k)}$ cease to change significantly

K. Evaluation Mechanism

In this section the performance of our proposed GFT-BPANN approach is studied through quantitative evaluation. The following evaluation models were chosen as quantitative scheme [4]:

(i) False Rejection Rate (FRR) as in (13).
(ii) False Acceptance Rate (FAR) as in (14).

False Rejection Rate (n) is defined as probability of number of rejected verification attempts of an authorized person N_{RA} to number of all verification attempts by an authorized person N_{AAP}. The values are better with more than independent attempt per person/feature.

$$FRR(n)=\frac{N_{RA}}{N_{AAP}}. \quad (13)$$

False Acceptance Rate FAR (n) is defined as the probability of the number of successful attempt imposter's fingerprint N_{SA} against a certain enrolled person to the number of all imposter attempts against a certain enrolled person N_{AIA}.

$$FAR(n)=\frac{N_{SA}}{N_{AIA}} \quad (14)$$

All these equations are used as objective evaluation schemes for degraded and fingerprints matching.

IV. Experiment and Results

One of the objectives of this paper is to apply the theory of our approach in practice to reduce the degradation and false minutiae in fingerprint image for authentication. The database of fingerprint images was created. The fingerprint images were captured using a Futronic fingerprint scanner.

DOI: 01.IJSIP.4.3. 1316

Hundred (100) good fingerprint images were enrolled into the database.

A second set of the same Hundred (100) fingerprint images were captured but without consideration of their state, these were then used as query fingerprint images. Some samples of the fingerprint images captured for querying the database are shown in Fig. 7 with various degree of degradation. Fifty (50) more fingerprint images were collected but were not part of the database. These fifty (50) fingerprint images where used as query to the database to measure FAR of our system. All of the second set fingerprint images were used as query fingerprint images to measure the FRR of the system. The system was implemented using MATLAB 7.

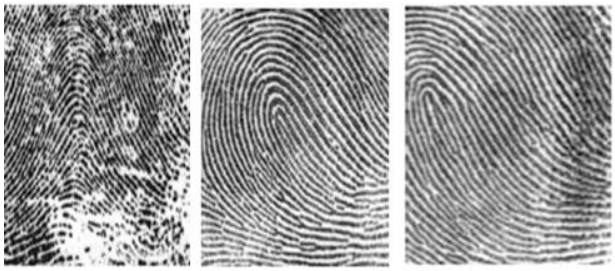

Figure 7: Samples of query Fingerprint Images captured for the experiment

A.Experiment 1: authenticate 2nd set of query fingerprint with the fingerprint templates in our fingerprint database

The experiment 1 to authenticate all the 2nd set of hundred (100) fingerprint images against the hundred (100) fingerprint images in the database to determine the FRR performance of the system. The fifty (50) fingerprint images that not in database are queried to measure the FAR of the system.

B.Experiment 2: authenticate the enhanced 2nd set of query fingerprint with the fingerprint templates in our fingerprint database

The experiment 2 is to enhance all the 2nd set of hundred (100) fingerprint images and then authenticate them against the hundred (100) fingerprint images in the database to determine the FRR performance of the system. The fifty (50) fingerprint images that are not in database are enhanced and then queried to measure the FAR of the system.

C.Experiment 3: authenticate the enhanced 2nd set of query fingerprint with the enhanced fingerprint templates in our fingerprint database

The experiment 3 is to authenticate the enhanced 2nd set of hundred (100) query fingerprint images against the enhanced database fingerprint templates in the database to determine the FRR performance of the system. The enhanced fifty (50) fingerprint images are queried against the enhanced database fingerprint templates to measure the FAR of the system.

D. Result

The results of enhancing a degraded fingerprint using Gabor filter can be seen in Fig 8. The top fingerprint image shows the original image and rectangle indicates a degraded section of the image. When Gabor filter was applied the bottom fingerprint image was obtained and rectangle indicates the repaired section of the degraded part.

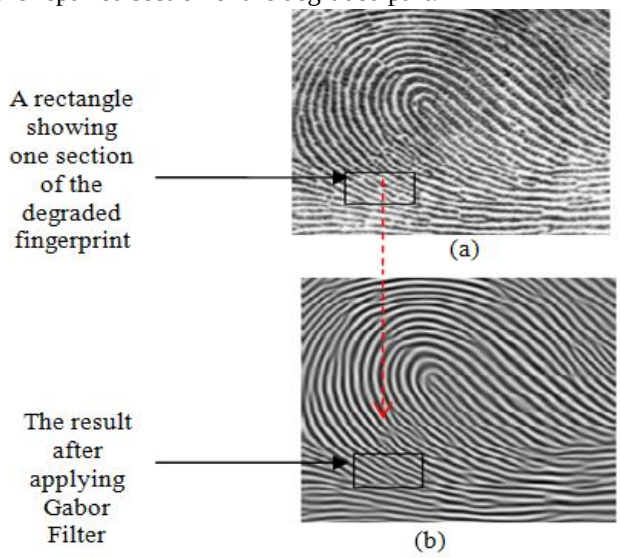

Figure 8. (a) is a distorted fingerprint image (b) is the result of applying Gabor Filter to the original distorted fingerprint image

From Fig 8, one can see the distorted fingerprint in Fig. 8(a) and when the propose GFT-BPANN approach is applied Fig. 8(b) shows the result an enhanced distorted fingerprint image.

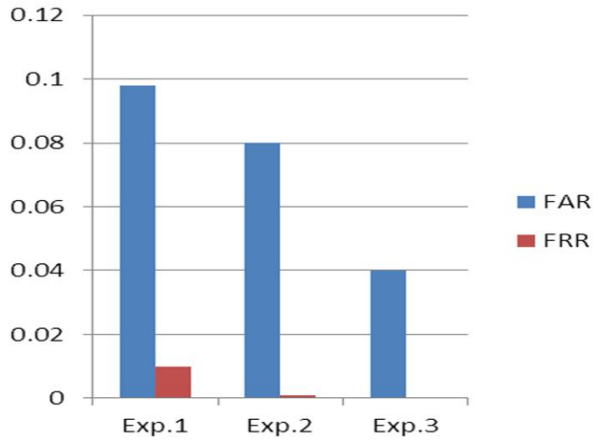

Figure 9: Experimental result for FAR and FRR

From Fig. 9, one can see the FAR and FRR of the experiment 1-3 which shows that the proposed approach has improved the performance of the biometric authentication system so much that in experiment 3 there was zero percentage FRR after enhancement.

V. Conclusions

In this paper we have discussed about fingerprint enhancement technique and also the back propagation technique for matching with the advantage of improving matching performance in case the feature on fingerprint has degraded and also to reduce authentication time search rate in a larger database. Another advantage of this approach is the ability to remove false minutia before matching. The experiments show that the performance of the system

DOI: 01.IJSIP.4.3.1316

improved so much that in experiment 3 there was zero percentage FRR after enhancement.

In future work the research can be explored further in different forms, including the following (i) using hierarchal for matching (ii) integrating multi-biometric for user authentication (iii) developing an algorithm for securing template fingerprint.

Acknowledgments

The authors acknowledge the financial support of Tshwane University of Technology.

References

[1] M.M. Abd AllahLL, "Artificial Neural Network Based Fingerprint Authentication With cluster algorithm". Informatica vol.9, pp 303-307, 2005.

[2] A. Almansa, and T. Lindeberg, "Fingerprint Enhancement Shaped Adaptation of Scale-Space Operators with Automatic Scale Selection". IEEE transaction on image processing vol.9, No.4, 2000.

[3] J. Cheng and J. Tian, "Fingerprint enhancement with dyadic scale-space". Pattern recognition Letters vol. 25, 2004. pp 1273-1284.

[4] A. EL-Sisi, "Design and Implementation Biometric Access Control System using Fingerprint for Restricted Areas Based on Gabor Filter", International Arab Journal of Information Technology, vol.8, No,4. 2011.

[5] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluations", IEEE transactions on pattern analysis and machine intelligence. vol.2, pp 777-789, 1998.

[6] X. Jiang, W.Y. Yau, and W. Ser, "Detecting the fingerprint minutiae by adaptive tracing the grey-level ridge", Pattern Recognition 34, pp. 999-1013. Center for signal Processing. Nanyang Technological University, Singapore, 2001.

[7] Y. Jiang, L. Liu, T. Jiang, and Y. Fan "A modified Gabor filter design method for fingerprint image enhancement", National Laboratory of pattern Recognition.1805-1817, pp 24, 2003.

[8] S. Khalil, "A back propagation Neural Network for Computer Network Security", Journal Computer Science 2(9):710-715, ISSN 1549-3636, 2006

[9] A.R. Kharade and M.S. Kumghar, "An identity-Authentication System using Fingerprint", International journal for Engineering Research and Application ISSN: 2248-9622, 2012.

[10] S.S Ponnarasi and M. Rajaram, "Impact of Algorithms for the Extraction of minutiae Points in Fingerprint", Journal for Computer Science, vol 8(9), pp 1467-1471,2012.

[11] M. Sepasian, W. Balachandran And C. Mares, "Image Enhancement for Fingerprint Minutiae-Based Algorithms Using CLAHE Standard deviation Analysis and Sliding Neighborhood" Proceedings of the World congress on Engineering and Computer Science 2008.

[12] J.W. Yang, L.F. Liu, and T.Z. Jiang, "Efficient Fingerprint Matching algorithm for Integrated circuit Cards", Journal computer Science and Technology, vol.19, No.4, pp 510-520, 2004.

[13] F. Zhao and X. Tang, "Pre-processing and Post processing for Skeleton-based Fingerprint Minutiae Extraction", pattern Recognition . vol.40, pp 1270-1281, 2007.

[14] M.A. EL-Iskandarani, H.M and Abdul-Kader, "Biometric. Authentication System using Fingerprint based on Self-organizing Map Neural Network Classifier", Alexandra Engineeriong Journal, vol. 44, No.5. 2005.

[15]S. Greenberg, and D. Kogan, "Fingerprint Image Enhancement using Filtering Techniques, Segmentation and Pattern Recognition", pp. 495-514.ISBN 987-3-902613-05-9. 2007.

[16] R. Rajkumar, and k. Hemachandran, "A secondary Fingerprint Enhancement and Minutiae Extraction, signal & image process", An International journal (SIPIJ) vol.3, No. 2. 2012.

[17] O.A Esan, T. Zuva, S.M Ngwira, and K. Zuva, "Performance Improvement of Authentication of Fingerprint using Enhancement and Matching Algorithm", International Journal of Emerging Technology and Advanced Engineering, vol. 3, issue 2, ISSN 2250-2459, 2013.

DOI: 01.IJSIP.4.3. 1316